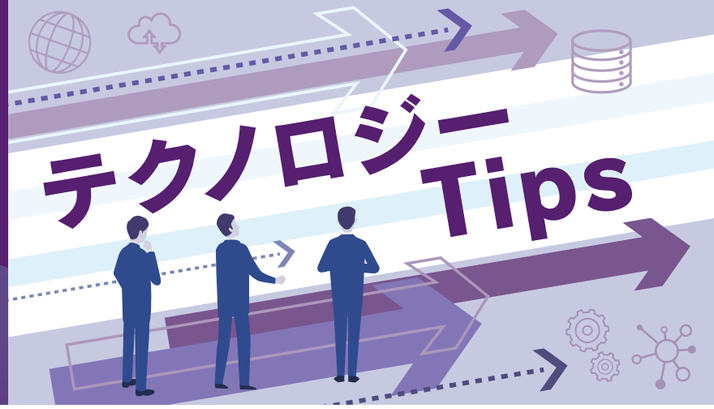
パスワード、数もやることも多すぎませんか？

長く、複雑に、使い回さず…とルールは増える一方で、現場はどんどん混乱していきます。実は、その混乱こそが、抜け漏れ・情報漏洩の入口になっています。

強固にすべきなのは分かる。でも、正直めんどくさい。長さ？多要素？…その「面倒」、仕組みで解決します。

パスワードは、会社の情報を守る「玄関の鍵」です。ところが今、その鍵1本だけでは家を守りきれない時代になりました。今回は、MFA・パスワードマネージャー・パスキーといった最新の対策と用語を基本から整理し、明日から何をすればよいかを順番に解説します。



1. なぜ今、パスワードだけでは守れないのか

かつては「複雑なパスワードを作れば安全」でした。しかし今は事情が違います。攻撃者は、漏れた大量のID・パスワードを世界中で売買し、機械で自動的に試してきます。1か所から漏れれば、同じパスワードを使っている他のサービスまで芋づる式に破られます。
だからこそ、考え方の出発点になるのが「認証の3要素」です。
本人確認の材料には次の3種類があり、これらを組み合わせるほど守りは固くなります。

知識情報	所持情報	生体情報
本人だけが知っている（パスワード、暗証番号）	本人だけが持っている（スマホ、専用の鍵）	本人自身の身体（指紋、顔）

パスワードは、このうち「知識情報」1つだけ。
だから、もう1種類を足すのが今の常識です。

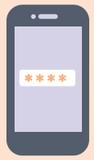
2. 守りを一段上げる ― MFA（多要素認証）

MFA（多要素認証）とは、ログイン時に前述の3要素のうち2種類以上を求める仕組みです。パスワードを盗まれても、手元のスマホがなければ入れないので、被害を大きく防げます。2FA（二要素認証）は、MFAのうち2種類を使うものを指します。なぜスマホを1つ足すだけで安全になるのでしょうか。パスワードは「知っている情報」なので、漏れれば誰でも使えてしまいます。しかしスマホに届く承認や生体認証は「持っている・本人である」情報で、遠くにいる攻撃者には再現できません。たとえパスワードが盗まれても、攻撃者の手元には肝心のスマホがない――この「別の種類の壁」がもう1枚あるだけで、乗っ取りの成功率は大きく下がります。自動化された攻撃多くは、MFAを有効にするだけで止められます。ここで大事な注意点です。「二段階認証」と「多要素認証」は似て非なるものです。
パスワードの後に「秘密の質問」を聞くのは、段階は2つでも、どちらも“知識情報”なので本当の多要素ではありません。
別の種類を足してこそ意味があります。

ワンタイムパスワード（OTP）

1回限りの使い捨て番号。使うたびに変わる。

認証アプリ（TOTP）



スマホアプリに30秒ごとに表示される番号。SMSより安全。

セキュリティキー

USBなどの物理的な鍵。最も強力な部類。

生体認証

指紋・顔で本人確認。スマホの標準機能でも使える。

3. 管理をラクにする ― パスワードマネージャー／SSO／IDaaS

「MFAも使い回し禁止も分かった。でも数十個も覚えられない」――その悩みを解くのが、管理の仕組みです。
この3つは似ていて混乱しがちなので、役割の違いから整理します。ざっくり言えば、パスワードマネージャーは「たくさんのパスワードを安全に持つ道具」、SSOは「そもそもログインの回数を減らす仕組み」、IDaaSは「それらを会社全体でまとめて管理するサービス」です。

パスワードマネージャー（まずは個人で）

サービスごとに違う長いパスワードを暗号化して保管し、強力なパスワードの自動生成・自動入力もしてくれる専用ツール。

利用者が覚えるのは「マスターパスワード」1本だけ。ブラウザの保存機能より安全性・機能が高く、業務では有償の専用ツールを推奨します。「使い回しをやめたいが覚えられない」を解決する道具です。

SSO（シングルサインオン）

1回のログインで、連携した複数のサービスに入れる仕組み。マネージャーが「鍵をたくさん安全にしまう」のに対し、SSOは「玄関を1つにまとめて鍵の数そのものを減らす」考え方です。入口が1つになるぶん、そこをMFAで固めれば全体の守りが一気に上がります。

IDaaS

このSSOとMFA、そしてID管理をクラウドでまとめて提供するサービス。社員の入社・退職に合わせてアカウントを一括で作成・停止でき、退職者アカウントの放置も防げます。個人の工夫（マネージャー）から全社の仕組み（IDaaS）へ、が自然な流れです。

併用が基本（ここが混乱ポイント）

SSOとパスワードマネージャーはどちらか一方ではなく「併用」が基本です。主要サービスはSSOで束ね、対応していない残りをマネージャーで守る。SSOの入口はMFAやパスキーで必ず固めるのが条件です。

4. パスワードの「次」— パスキー（パスワードレス認証）

いま最も注目されているのがパスキー（Passkey）です。
パスワードそのものを使わず、スマホやパソコンの生体認証で本人確認する新しい方式で、対応するサービスが急速に増えています。パスワードが存在しないため、盗む・使い回す・忘れるという問題が根本からなくなり、後述するフィッシングにも強いのが特長です。
すぐ全部を切り替える必要はありませんが、対応済みのサービスから順にパスキーへ、が次の一歩です。

Column 強いパスワードを“作る”なら

パスワードを使う場面では、複雑さより「長さ」が重要です。記号を混ぜた8文字より、覚えやすい単語をつないだ16文字以上（パスフレーズ）の方が、はるかに破られにくくなります。下の表は、漏れたパスワードを攻撃者が手元で解析した場合の解読時間の目安です。ただし、どれだけ長くても使い回しや辞書にある単語は数秒で破られます。長さとランダムさ、この2つが決め手です。

パスワードの作り方	解読までの目安	解読の難しさ（イメージ）
8文字・小文字だけ	約2週間	■■□□□□□□
8文字・英大小＋数字＋記号	約132年	■■■■□□□□
13文字以上・英大小＋数字＋記号	数千年以上（事実上不可能）	■■■■■■■■
使い回し／辞書にある単語	長さに関係なく数秒	■！□□□□□□

※出典④：Hive Systems「2026 Password Table」。攻撃者が漏れたデータを手元で解析した場合の最大時間の目安・ランダム生成が前提。

5. やってはいけないパスワード管理【最重要】

ここが事故の温床です。次の6つは今日からやめてください。

① 使い回し	最悪の習慣。1か所の漏洩を突いて他サービスへ自動ログインを試す「クレデンシャルスタッフィング攻撃」の標的になります。
② 付箋・共有ファイルでの平文保存／アカウントの共有	誰が使ったか分からず、退職時に回収もできません。
③ 単純な文字列（123456、password、社名、誕生日）	辞書攻撃で真っ先に破られます。
④ 定期的な強制変更	実はこれ、今は非推奨です。定期変更を強いると、人は「Pass01→Pass02」のように単純化・使い回しに走り、かえって弱くなるためです。総務省も2024年5月に指針を見直し、流出などの兆候がある時だけ変更すればよいと明記しています（出典①）。米国のNISTも同様の方針です（出典②）。
⑤ SMSだけに頼った認証	番号を乗っ取る手口があり、NISTはSMS方式を「利用制限すべき」と位置づけています（出典②）。使うなら認証アプリやセキュリティキーへ。
⑥ MFAがあるからと油断する	パスワードとMFAを突破する「AiTM（中間者型フィッシング）」が急増しています。偽サイトを経由させ、ログイン後の“通行証”を丸ごと盗む手口で、Microsoftは2024年に前年比146%増と報告しています（出典③）。怪しいリンクは踏まない、が最後の砦です。

よくある被害イメージ

CASE 1 使い回し

ある会社では、社員が私用でも使っていたパスワードを、業務システムでも使い回していました。私用で登録していたあるサービスが情報漏洩を起こし、流出したID・パスワードの一覧を使って業務システムに侵入され、取引先情報が抜き取られました。パスワード自体は複雑でしたが、「使い回し」という一点だけが原因でした。

CASE 2 MFA過信

別の会社では、MFAを設定していたにもかかわらず被害に遭いました。取引先を装ったメールのリンクから偽のログイン画面へ誘導され、ID・パスワードとワンタイムコードをそのまま入力。攻撃者はそれを即座に本物のサイトへ転送してログイン後の通行証を盗み、正規の利用者になりすましました。設定していれば安心、ではなく「怪しいリンクを開かない」までがセットです。

6. 今日からやること — 順番に進めればOK

一度に全部は無理です。
初心者→中級の順で、着手してください。

【中級：仕組みで守る】

⑥ 対応済みのサービスからパスキーへ順次移行する。

⑤ 退職者・管理者アカウントを棚卸しし、不要なものを停止する。

④ 全社でSSO／IDaaSを検討し、ログインの入口を1つに集約してMFAで固める。

【初心者：まずここから】

③ 付箋・Excel管理をやめ、パスワードマネージャーを1つ導入する。

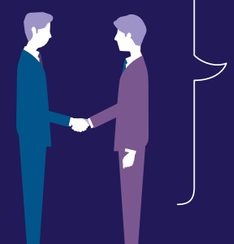
② 重要サービスにMFAをオンにする（設定画面に必ずあります）
SMSより認証アプリを選ぶ。

① 使い回しをやめる。
特に「メール」「銀行」「業務システム」の重要3つは、それぞれ別の長いパスワードに。

最後に パスワードは「長く・使い回さず・もう一つの鍵（MFA）を足す」

この3点さえ押さえれば、守りは一気に固くなります。難しく考えず、重要な3サービスから、今日始めてみてください。

長く 十分な長さのパスワード ＋ **使い回さず** サービスごとに別パスワード ＋ **もう一つの鍵（MFA）** MFA（多要素認証）を必ず使う

出典 ① 総務省「国民のためのサイバーセキュリティサイト」安全なパスワードの設定・管理（2024年5月刷新）② NIST SP 800-63B Rev.4（2025年8月最終化）— 定期変更の強制禁止、SMS認証の利用制限
③ Microsoft報告（2024年、AiTM攻撃 前年比146%増）④ Hive Systems「2026 Password Table」— パスワード長・複雑さ別の解読時間目安（bcrypt・レンタルGPUでの最大時間）

ぜひ、ご相談ください！
御社のAI×DX伴走パートナーであり続けます。